BÀI THỰC HÀNH SỐ 3

**Phân tích kịch bản tấn công DNS Cache Poisoning**

1. **Giới thiệu chung**
   1. **Mục đích**

Dịch vụ phân giải tên miền DNS được triển khai để tìm kiếm thông tin về một tên miền trên mạng Internet. Quá trình này thường diễn ra khi một chương trình client chỉ biết tên miền của máy chủ mà không biết địa chỉ IP của máy chủ đó. Có nhiều cách khác nhau để can thiện vào quá trình này nhằm sửa đổi thông tin trả lời từ máy chủ phân giải tên miền. Trong đó, tấn công DNS Cache Poisoning thực hiện tới mục tiêu là các máy chủ DNS nhằm đưa thông tin giả mạo vào trong bộ đệm dịch vụ của nạn nhân. Hậu quả của tấn công này là tất cả các máy yêu cầu nhận được kết quả là một địa chỉ giả mạo và do đó các chương trình client sẽ truy cập vào máy chủ giả mạo.

Bài thực hành này được thiết kế để sinh viên thử nghiệm kỹ thuật tấn công được đề xuất bởi Kaminsky và phân tích đặc điểm của kỹ thuật này.

* 1. **Môi trường thực hành**
* Hệ điều hành: Linux Ubuntu
* Các công cụ: Docker, Wireshark, Python
  1. **Chuẩn bị thực hành**
* Đọc lại bài giảng và các tài liệu về tấn công DNS Cache Poisoning
* Đọc tài liệu thực hành
* Hoàn thành đúng >50% số câu hỏi trắc nghiệm chuẩn bị thực hành
* Luyện tập sử dụng các công cụ trong bài thực hành

1. **Một số thao tác căn bản với Docker**

Môi trường thực hành được triển khai trên các máy ảo Linux Ubuntu trong Docker được gọi là container. Các container này được thi trên một máy chứa gọi là host. Sau đây là một số lệnh thao tác căn bản cần sử dụng trong bài thực hành:

* Xây dựng các container: $ docker-compose build
* Khởi động các container: $ docker-compose up

Có thể tắt container bằng cách nhấn tổ hợp phím Ctrl + C nhưng file ảnh (image) của container không bị xóa.

* Tắt container và xóa file ảnh: $ docker-compose down
* Liệt kê các container: $ dockps
* Truy cập và thực thi lệnh shell trên container: $ docksh <container\_id>

Trong đó <container\_id> chỉ cần một vài ký tự đầu tiên trong ID của container. Có thể mở nhiều cửa sổ Terminal để kết nối tới cùng một container.

* Khởi động lại container: $ docker restart <container\_id>
* Sao chép file từ máy host sang thư mục /tmp trên Docker container

docker cp <file\_on\_host> <container\_id>:/tmp

* Sao chép file từ thư mục /tmp trên Docker container sang máy host

docker cp <container\_id>:/tmp/<filename> <file\_on\_host>

* Bắt gói tin trong mạng ảo hóa của Docker bằng Wireshark: chọn cạc mạng bắt đầu bằng **br-**

Graphical user interface, text, application

Description automatically generated

* Bắt gói tin trong máy ảo container và lưu lại

# tcpdump -i eth0 -n -w <file\_name.pcap>

1. **Tổ chức thực hành**

* Sinh viên làm bài thực hành theo nhóm đã phân công.
* Mỗi nhóm thực hiện các kịch bản tấn công đã mô tả sau đây.
* Mỗi nhóm viết báo cáo theo mẫu dựa trên kết quả thực hiện các kịch bản tấn công

Trên máy tính tại phòng thực hành, các bạn được cung cấp một máy ảo VM chạy hệ điều hành Ubuntu 20.04 trong phần mềm ảo hóa Virtualbox. Máy ảo VM này đóng vai trò là máy chứa (host) cho các Docker container. Các kịch bản tấn công được thực hiện trên mạng ảo hóa bằng Docker như sau:

Diagram

Description automatically generated with medium confidence

Trong bài thực hành này, chúng ta sẽ thử nghiệm một kịch bản tấn công DNS Cache Poisoning dựa trên kỹ thuật của Kaminsky như sau:

1. Máy tấn công Attacker gửi một thông điệp DNS Query tới máy nạn nhân Local DNS Server, yêu cầu phân giải tên miền không tồn tại trong **example.com**
2. Khi không có thông tin về tên miền được truy vấn, máy nạn nhân gửi truy vấn tới máy chủ gốc (root server) trong cây phân cấp tên miền
3. Trong khi máy nạn nhân chờ trả lời, máy tấn công gửi một lượng lớn các thông điệp DNS Response giả mạo, cung cấp thông tin bản ghi NS cho biết máy chủ **ns.attacker32.com** là máy chủ tên miền của **example.com**.
4. Nếu có thông điệp DNS Response giả mạo hợp lệ đến trước thông điệp DNS Response tin cậy, tấn công thành công. Ngược lại, lặp lại từ bước 1 với một tên miền không tồn tại khác của example.com
5. **Nội dung thực hành**
   1. **Triển khai hệ thống (1 điểm)**

* **Bước 1:** Trên máy host, truy cập vào thư mục ~/it4263lab/lab03
* **Bước 2:** Mở filedocker-compose.yml. Sửa thông số địa chỉ IP cho các container với x là 2 số cuối trong mã lớp thực hành, y là số thứ tự của nhóm.
* **Bước 3:** Mở file image\_attacker\_ns/zone\_attacker32.com và sửa địa chỉ IP trong các ánh xạ theo quy ước trên.
* **Bước 4:** Mở file image\_attacker\_ns/zone\_example.com và sửa địa chỉ IP trong ánh xạ ns theo quy ước trên
* **Bước 5:** Mở file image\_local\_dns\_server/named.conf và sửa địa chỉ IP trong forwarders theo quy ước trên.
* **Bước 6:** Mở file image\_user/resolv.conf và sửa địa chỉ IP của name server theo quy ước trên.
* **Bước 7:** Xây dựng các container cho bài thực hành và khởi động chúng
* **Bước 8:** Truy cập vào các container để thực thi các lệnh shell.
* **Bước 9:** Kiểm tra kết nối giữa các máy ảo container bằng lệnh ping
* **Bước 10:** Trên máy host, sử dụng Wireshark để bắt lưu lượng trong mạng ảo của các container.

**Kiểm tra hoạt động của dịch vụ DNS từ máy User**

* **Bước 11:** Trên máy User, thực hiện lệnh tìm kiếm tên miền **ns.attacker32.com**. Ghi nhận kết quả vào báo cáo.

**# dig ns.attacker32.com**

* **Bước 12:** Trên máy User, thực hiện lệnh tìm kiếm tên miền **www.example.com**. Ghi nhận kết quả vào báo cáo.

**# dig www.example.com**

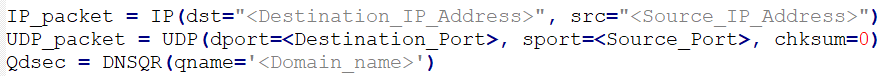
* **Bước 13:** Trên máy User, thực hiện lệnh tìm kiếm tên miền **www.example.com** trên máy chủ Attacker Server. Ghi nhận kết quả vào báo cáo.

**# dig @ns.attacker32.com www.example.com**

* 1. **Tạo thông điệp DNS Query truy vấn (2 điểm)**

Trong phần này, các bạn cần tạo ra thông điệp DNS Query truy vấn một tên miền không tồn tại trong example.com

* **Bước 1:** Truy cập thư mục ~/it4263lab/lab03/attack
* **Bước 2:** Mở file **gen\_query.py** và sửa các thông số cần thiết để tạo yêu cầu truy vấn tên miền tới máy chủ nạn nhân Local DNS Server.



* **Bước 3:** Thực thi **gen\_query.py** trênmáy Attacker**.** Sau khi thực thi xong, file **ip\_req.bin** được sinh ra với nội dung là một thông điệp DNS Query như đã đề cập
  1. **Tạo thông điệp DNS Response giả mạo (2 điểm)**

Trong phần này, các bạn cần tạo ra thông điệp DNS Response cung cấp thông tin giả mạo về máy chủ tên miền của example.com như kịch bản đã mô tả.

* **Bước 1:** Truy cập thư mục ~/it4263lab/lab03/attack
* **Bước 2:** Mở file **gen\_response.py** và sửa các thông số cần thiết để tạo thông điệp DNS Response giả mạo trả lời cho máy chủ nạn nhân Local DNS Server.

A picture containing scatter chart

Description automatically generated

*Lưu ý:*

* *Để kịch bản tấn công thực hiện dễ dàng hơn, máy chủ Local DNS Server luôn sử dụng số hiệu cổng ứng dụng 44444 để gửi yêu cầu DNS Query*
* *Sinh viên cần phải xác định địa chỉ của máy chủ tên miền gốc (root server) mà Local DNS Server gửi yêu cầu truy vấn tới đó. Phân tích lưu lượng bắt được trong phần 4.1 để tìm thông tin này.*
* **Bước 3:** Thực thi **gen\_response.py** trên máy Attacker**.** Sau khi thực thi xong, file **ip\_resp.bin** được sinh ra với nội dung là một thông điệp DNS Query như đã đề cập
  1. **Thực hiện tấn công DNS Cache Poisoning (4 điểm)**

Trong phần này, để cuộc tấn công hiệu quả hơn, các bạn đã được cung cấp file **attack.c** để tự động thực hiện kịch bản tấn công đã mô tả. Khi thực thi, các file chứa thông điệp DNS Query và DNS Response đã tạo ra ở bước 4.2 và 4.3 sẽ được nạp vào.

* **Bước 1:** Biên dịch file **attack.c** trên máy host thành file thực thi có tên là **attack**

**$ gcc attack.c -o attack**

Sao chép file thực thi tấn công vào máy Attacker.

* **Bước 2:** Trên máy Attacker, thực hiện bắt lưu lượng mạng
* **Bước 4:** Trên máy Local DNS Server, thực hiện bắt lưu lượng mạng
* **Bước 4:** Trên máy Attacker, truy cập vào thư mục chứa file **attack** thực thi tấn công. Thực thi lệnh **# ./attack** để tấn công
* **Bước 5:** Trên máy User, thực hiện các lệnh tìm kiếm thông tin tên miền sau:

**# dig www.example.com**

**# dig @ns.attacker32.com www.example.com**

Nếu kết quả của hai tìm kiếm này cùng cho thấy máy chủ tên miền **example.com** là ns.attacker32.com thì tấn công đã thành công. Ngược lại, thực hiện lại tấn công với một truy vấn tới tên miền không tồn tại khác của example.com.

* **Bước 6:** Trên Local DNS Server, thực hiện lệnh sau để trích xuất nội dung bộ đệm dịch vụ

**# rndc dumpdb -cache /var/cache/bind/dump.db**

* **Bước 7:** Dừng tấn công. Dừng bắt lưu lượng trên các máy và đặt tên các file lưu lượng lần lượt là **attacker.pcap** và **local\_dns\_server.pcap**

Viết báo cáo quá trình thử nghiệm tấn công theo mẫu.

* 1. **Phòng chống tấn công (1 điểm)**

Một trong những cách thức đơn giản để phòng chống tấn công DNS Cache Poisoning là thực hiện cấu hình để máy chủ DNS sử dụng một cổng dịch vụ ngẫu nhiên để gửi thông điệp DNS Query đi.

* **Bước 1:** Kết nối với máy ảo container Local DNS Server để thực thi lệnh shell
* **Bước 2:** Mở file named.conf.options để sửa

**# nano /etc/bind/named.conf.options**

* **Bước 3:** Xóa dòng sau trong file trên

query-source port 44444;

* **Bước 4:** Nhấn Ctrl+O để lưu lại file.
* **Bước 5:** Nhấn Ctrl + X để đóng file. Khởi động lại container của máy chủ Local DNS Server

Thực hiện lại tấn công để kiểm nghiệm kết quả